LAUR-99-4821

TAMPER-INDICATING SEALS
FOR NUCLEAR DISARMAMENT AND HAZARDOUS WASTE MANAGEMENT

Roger G. Johnston[a]

[a] Team Leader, Vulnerability Assessment Team, Los Alamos National Laboratory

MS J565, Los Alamos National Laboratory, Los Alamos, NM 87545 USA

Phone: 505-667-7414 fax: 505-665-4631 email: rogerj@lanl.gov

ABSTRACT

Tamper-indicating seals have important applications in many areas, including nuclear disarmament and hazardous waste management. There are, however, many theoretical and practical problems with current seals and seal usage, as well as with tamper detection in general. Most current seals appear to be highly vulnerable to simple and rapid attacks, although this can change with improvements to the seals or to how they are used. Few seals appear to be designed with disarmament and waste management applications in mind. Better seals are possible, especially if new approaches and technologies can be exploited. Seals based on sophisticated technology, however, do not automatically provide better security.

INTRODUCTION

Tamper-indicating seals, often called “security seals” or simply “seals”, are designed to record unauthorized access or entry. Seals are widely used for many different applications. These include access control, records integrity, inventory and cargo security, theft prevention and detection, hazardous materials accountability, nuclear nonproliferation/safeguards & security, law enforcement, customs, counterterrorism, counterespionage, and tamper-evident packaging for consumer products.

Seals have been used for thousands of years. The general field of tamper detection is nevertheless relatively undeveloped and hampered by problems. There exists no formal theory of tamper detection, nor is there much in the way of meaningful, comprehensive standards[1]. Few seal users have a sophisticated understanding of how to choose seals, how to best use them, or the nature of their vulnerabilities[2].

Many of the seals currently in use (including for nuclear applications) lack key attributes needed for effective transparency, negotiability, and security for international arms reduction treaties. Opportunities and technologies for new, more effective seals have been underutilized. In the case of hazardous waste management, the potential benefits of seal use have often been ignored. Indeed, few seals are even optimized for waste management applications.

The purpose of this paper is to review the status of tamper-indicating seals, and to suggest some of the required attributes for international arms control and for hazardous waste management. A secondary purpose is to highlight the current problems with seals and to speculate on future developments.

TERMINOLOGY

One of the problems that complicates seal use is widespread ambiguity about the definitions and separate functions of locks, seals, and tags.

For our purposes, a **seal** (or **tamper-indicating device**) is defined as a device or material designed to leave unerasable evidence of unauthorized access. A seal does not need to provide resistance to entry; it need only record that it took place. Some seals are made of paper or plastic and can be easily torn open with the fingers. This does not necessarily make them ineffective.

A **lock**, in contrast, is hardware designed to delay and complicate unauthorized entry or access. Locks do not substantially impede adversaries who are sufficiently motivated and/or skilled.

A **barrier seal** is a single device that performs the functions of both a lock and a seal. It typically can withstand considerable force without opening. A barrier seal is usually a compromise--less than the optimum seal and less than the optimum lock for any given application.

A **tag** is an intrinsic or applied unique characteristic ("fingerprint") used to unambiguously identify an object or container.

Other relevant terms of interest include:

defeating a seal: gaining entry or access through the seal to what the seal is protecting without being detected.

attacking a seal: trying to defeat it.

seal protocols: the official and unofficial procedures for seal procurement, transport, storage, check-out, record keeping, installation, inspection, removal, disposal, and training of personnel. The effectiveness of a seal depends critically on the protocols used with it.

seal inspection: checking a seal for signs of tampering, counterfeiting, or evidence of unauthorized entry. Unlike locks, seals must be inspected (by man or machine) in order to provide security.

postmortem exam: a careful study of seal parts after the seal has been used, removed, and inspected in the field. This forensic analysis may involve sophisticated laboratory methods to determine if there has been tampering, or if the seal has been attacked or counterfeited.

vulnerability assessment: finding (and perhaps demonstrating) the weaknesses in the design and execution of a security device or security program, often accompanied by suggested counter-measures.

EARLY SEALS

Seals have been in use for at least 7,000 years, well before the invention of writing[3]. Indeed, some scholars think seals encouraged the development of both writing and arithmetic[4].

A typical ancient seal consisted of a small cylinder or stamp made of clay, wood, stone, or bone, and carved with a geometrical or complex design. Containers such as pots or jugs were secured by placing clay over the lid, mouth, cap, or stopper. The stamp or cylinder seal was then used to impress a pattern into the clay, either by pressing the stamp seal, or by rolling the cylinder seal along the clay. The clay was allowed to harden, perhaps by baking in the sun. Any attempt to open the container would presumably require fracturing the clay. Replicating the pattern to reseal the container (and hide the fact that it had been opened) would require significant time and skill if the trespasser did not possess the original seal. Alternatively, a cord could be tied around a container, package, bundle, or door. A bulla (lump of clay) was then placed around the knot, prior to pressing the seal design into the clay.

Another ancient use for seals was for documents. Written clay tablets from 5000 B.C. onward were often imprinted with the design from a stamp or cylinder seal. This was a tag-like signature to authenticate the document and identify the author. The clay tablet might also be sealed inside a clay envelope, which was impressed with a seal design to detect tampering.

The Egyptians were using bullae to seal papyrus documents by 2500 B.C. They also used seals on the tombs of their dead. When the burial chamber was completed and the mummified body placed inside, the door was sealed with mud and plaster. The door could still be opened, but it would then be obvious that the seal was broken. In modern times, archaeologists were able to tell if a tomb had been looted by checking to see if the seal was intact.

From 1100 BC through medieval times, wax seals were widely used in Europe. Wax was melted and then dripped onto a scroll. (Shellac eventually replaced wax.) A signet ring--engraved with a distinctive design--was then pressed into the molten blob of wax, leaving behind the complex design. Lead seals were also in use from the 4th century A.D. to today[5].

Ancient, medieval, and Renaissance seals apparently offered less than absolute security. Evidence for this includes the discovery of counterfeit seals[3,6], and the problem of art forgers lifting seals from paintings in order to make forgeries[7].

MODERN SEALS

There are probably over 5,000 different seals in use today. These fall into two major categories: **passive** and **active**. A passive seal works without electrical power. Passive seals are usually meant for one-time use and are typically inexpensive. An active (or dynamic) seal is powered by electricity, either internally or externally. Active seals are typically reusable[8].

Passive seals take a variety of forms[9,10]. They can be frangible foils or films; plastic wraps; pressure-sensitive adhesive labels; “locking” bolts, crimped wires/cables, or other (theoretically) irreversible mechanical assemblies; tamper-evident packaging and security containers or enclosures that give evidence of being opened; fiber optic bundles that show changes in light transmission when cut; and other devices or materials that display irreversible damage or changes when manipulated.

Figure 1 shows an assortment of commercial passive seals; there is no particular significance to the ones chosen. All of the seals shown except the passive fiber optic seal and the two adhesive label seals are irreversible mechanical assemblies. When such a seal is closed, it "locks" in a manner similar to cable ties. At least in theory, these seals cannot then be opened without causing obvious damage. All the seals except the adhesive label seals are typically passed through a hasp before being closed. The loop size after the seal is closed can be adjustable or fixed, depending on the design. The adhesive label seals are frangible and are intended to become damaged when removed from a surface.

Active seals are usually of two types: electronic or (active) fiber optic. Electronic seals continuously monitor for some kind of change indicative of tampering. Active fiber optic seals periodically or randomly send light pulses down a fiber optic bundle to check continuity.

Most modern seals are still inspected manually, though some seals use an electronic or optical reader (verifier) to check for tampering.

SEAL VULNERABILITIES

Tamper-indicating devices currently in use both commercially and for government purposes appear to be vulnerable to rapid, simple, low-tech attacks. The most comprehensive study in support of this conclusion has been undertaken by the author and the Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory[1,2,11]. Others, however, have openly published reports and papers with similar conclusions[9,12]. There also appears to be an informal consensus among seal vulnerability assessors outside of the VAT that most or all seals are vulnerable to simple attacks.

The VAT studied 120 different seals in wide-spread use[11]. The seals included low- and high-tech devices, both passive and active. The VAT found that ALL 120 seals could be defeated using low-tech tools and methods available to the general public. The defeats would not be detected with the typical inspection protocols used with each type of seal. Defeat times for one, well-practiced individual ranged between 3 seconds and 2 hours, with the mean time being well under 5 minutes[13]. If we consider only those seals out of the 120 currently in use for U.S. or international nuclear applications, the mean defeat time (for one well-practiced individual) was under 8 minutes.

The average cost of an attack for all 120 seals was $55, though the marginal cost was much less[14]. Some high-tech seals could be defeated more easily than low-tech seals. The VAT also concluded that seal cost was not a good predictor of vulnerability[11].

One important finding was that simple changes to the seal and/or its use protocols can often dramatically improve tamper detection. The optimum protocols, however, depend critically on the specific seal being used and on details of the application.

PLAUSIBILITY OF SEAL VULNERABILITIES

It is not possible in this forum to provide the full evidence for seal vulnerabilities. Space is too limited to discuss specific vulnerabilities, plus it would be irresponsible to disseminate information on how to defeat tamper indicating devices. Instead, we can consider 6 arguments for why the idea that seals can be defeated should be both plausible and unsurprising.

The first argument is that all seals--at least in theory--can be counterfeited. The reasoning is based on the atomic theory of matter. All existing seals are composed of combinations of essentially identical electrons, neutrons, and protons. These basic building blocks are available in copious quantities at low cost. To counterfeit a seal, one needs “merely” to assemble these basic components in approximately the correct configuration[15]. The original seal can be cut off and replaced with the resulting counterfeited seal without leaving any evidence. In practice, of course, assembling the correct configuration of elementary particles or atoms may take enormous time, skill, and sophisticated technology. Nevertheless, there is nothing in our current understanding of physics that fundamentally prohibits replicating any man-made object, including a seal.

The second argument for the plausibility of seal vulnerabilities relies on the fact that counterfeiting has worked well for a wide variety of different objects. These include works of art, fossils, consumer products, antiquities, antiques, sports memorabilia, gem stones, official documents, IDs, and money[16]. Simple and low-tech methods often work remarkably well[16].

The third argument is based on the observation that there are many possible ways to attack a seal, in addition to counterfeiting. The VAT, for example, has compiled a taxonomy of 105 general methods for attacking seals[17]. These 105 generic attacks fall into 11 broad categories, described in Appendix A.

The fourth argument in support of seal vulnerabilities relies on the well known fact that locks (including electronic ones) can be quickly and thoroughly compromised. Information on how to defeat even sophisticated locks is readily available[18]. Now it is true that locks have a different security function. They are, nevertheless, installed in similar ways and are commonly used interchangeably with seals (though not always wisely). Unlike seals, however, locks have a simple binary status. They are either locked or unlocked[19]. If locks can be easily defeated, why should we expect seals to be any different, given that they require a much more subtle human or machine interpretation of their status, i.e., whether tampering has occurred? The human element is often particularly exploitable for purposes of defeating seals[17].

The fifth argument is actually a proposed experiment. If you obtain a seal and review how it is used, you will probably be able to conceive of multiple ways in which you can defeat it. Few seal users appear to have undertaken this mental exercise.

The sixth argument for seal vulnerability is based on the difficulty of proving a negative. If an attempt to defeat any given seal fails, that doesn't necessarily mean that the seal is undefeatable. It may simply mean that the wrong methods, personnel, and technology were employed for the attempt. Even making the assumption that a given seal is effectively undefeatable may be counter-productive since it can lead to overconfidence--a classic flaw in any security or verification program.

It is sometimes thought that defeating seals ought to be difficult because the attacker will be ignorant of the seal design or the seal serial number, right up to the time of the attack. In truth, however, there are few, if any, seals currently in use for nuclear applications that are unknown or unobtainable to outsiders prior to instigating an attack. Most seals in use for nuclear applications have been commercialized, or the design made publicly available. Even when this is not the case, it is not impossible to obtain samples of such seals (used or unused), either overtly or surreptitiously. For dismantlement treaties, of course, both sides will need to know the seal design in great detail from the outset, so making the assumption that an adversary will begin an attack ignorant of the nature of the seal is not valid.

Similarly, the fact that an adversary might not know the serial number of a given seal at the start of an attack is not usually going to impede counterfeiting. The seal will have been counterfeited without a serial number prior to the attack. For most seals, inserting the proper serial number into the counterfeit seal can be done quickly in the field; it is not usually the most difficult or time-consuming aspect of seal counterfeiting.

SEAL TRADEOFFS

The typical tamper-indicating seal has a tradeoff curve of the sort shown in figure 2. The ease of defeating the seal is shown plotted as a function of the amount of effort the seal users puts into using the seal. The effort is characterized in terms of "hassle"--a qualitative technical term commonly employed by the actual personnel who install and inspect seals[20].

Basically, figure 2 shows that if a seal user is willing to put up with a lot of hassle in using a seal, he can make it difficult for an adversary to defeat the seal. This hassle may require careful procedures for installing and inspecting the seal, as well as carefully quality control, record keeping, and training. If, on the other hand, the seal user is unwilling to devote considerable effort to using the seal, an adversary will find it easy to defeat. Thus, a modest seal used with great care can provide good tamper detection, while a sophisticated seal used poorly may not.

The large drop in the curve shown in figure 2 is due to the implementation of a postmortem exam. Few tamper detection programs incorporate one.

Based on the work of the VAT, high-tech seals or seals that are checked with a reader (verifier) tend to have a trade-off curve like that shown in figure 3. Compared to a more conventional low-tech seal, the high-tech or verifier-checked seal can provide better security than conventional seals--but only if the user devotes extra effort to using it. For low levels of effort, conventional seals tend to perform better. Unfortunately, many seal users choose high-tech seals or readers primarily because they want to reduce the work load for seal inspectors.

One of the common problems with high-tech seals or readers is the "Titanic Effect"--an overconfidence in high technology. With manual inspection of low-tech seals, seal inspectors are required to pay careful attention to the details of the scene they are examining. They thus have a good chance of detecting tampering or spotting suspicious anomalies. With high-tech seals and/or readers, however, seal inspectors tend to blindly trust what the seal or reader says (especially if they don't fully understand the technology), at the cost of being less observant of the overall scene. This can be readily exploited by an adversary. Furthermore, high-tech seals or readers give an adversary many more legs to attack than is the case for simpler seals.

CURRENT PROBLEMS WITH SEALS

There are a number of reoccurring problems with seals, how they are thought of, and how they are used. These problems exist across a wide range of applications and for many different types of seal users. Some of these problems have been mentioned above.

A fundamental problem with current seals is that, once tampering is detected, the seal may fail to permanently record it in an unerasable manner. If an adversary can erase or hide the evidence of entry, the seal is made ineffective. Improvements in this area are clearly needed, and are a current focus of new seal concepts under development at Los Alamos National Laboratory.

A particularly serious problem with the current use of seals is a common lack of effective training for seal installers and inspectors. The most effective countermeasures for seal attacks require an understanding of the specific seal's vulnerabilities and a familiarity with the most likely attack scenarios. The instructions typically given to seal inspectors, however, are to "look for signs of tampering". (This is true even for critical applications.) Information about EXACTLY what to look for is often missing. In the view of the VAT, seal inspectors should be shown examples of attacked seals. Even better, they should be shown how to attack the specific seals they are using, since this provides the most direct and useful information[21].

Equally ubiquitous is a widespread misunderstanding of seals testing. Vulnerability assessments are quite different from other types of tests, such as testing for seal suitability, ease of use, field readiness, strength, and environmental durability. Many seal users lump all types of testing into one category, and have unjustified confidence in the seal they are using if it manages to "pass" one type of test or other. The widespread desire among seal users to obtain some kind of certification for the seals they are using is also unhelpful[1]. Seal standards and the theory of tamper detection are not advanced enough to give meaning to certification. Furthermore, certification invariably involves over-simplifying important issues and glossing over critical details of the specific application of interest.

Yet another problem that impedes the effective use of seals is an improper attitude towards vulnerability assessments. In the minds of many seal users, a vulnerability assessment should find zero vulnerabilities. In reality, an effective vulnerability assessment must always find vulnerabilities (since they always exist); otherwise it has no value[1]. The discovery of vulnerabilities should be viewed as good news--because it means the seal's security can be improved--rather than bad news[22].

Some seal users dismiss the need for optimizing seal security because they use other layers of physical security in conjunction with seals. This may include fencing, locks, intrusion alarms, video surveillance, guards or guard dogs, 2- or 3-man rules for access to critical items, or careful screening of critical personnel.

Now it certainly is true that these measures can substantially improve security if used effectively. But other levels of security should never be used as an excuse to avoid optimizing seal effectiveness, especially if--as the VAT has found--it can often be done fairly easily. In any event, relying on other layers of security to overcome shortfalls in one particular layer can be dangerous. It tends to foster an attitude that we won't take seriously alarms or suspicious situations at one level because the other levels will back us up. Adding extra layers of unreliable security can sometimes actually decrease overall security, rather than improve it.

Multiple layers of security may also beg the question about the nature of an adversary. Facility insiders and treaty inspectors will already have gained access through multiple layers of security by the time they come face to face with a seal. Those outer layers may not, therefore, be fully relevant in evaluating seal security.

It is also possible that the security provided by video surveillance or 2- or 3-man rules is often overestimated. Few security personnel have training in observational skills, or in distraction and misdirection techniques. The latter can be remarkably effective when well executed--as any good magician can demonstrate. Also, the personnel in 2- and 3-man crews often form strong friendships and loyalties (even when randomly assigned) that may interfere with their objectivity in monitoring fellow crew members. In the case of international treaty monitoring, inspectors may be particularly vulnerable to distraction, misdirection, or observational errors due to jet lag, travel fatigue, cultural disorientation, intimidation, and work-related stress.

Another continuing problem with seals is that the seals market is driven primarily by commercial users who often appear more focused on unit cost than security[2]. The portion of the market represented by government and commercial users interested in high security is still relatively small. As a result, few seal developers and manufacturers concentrate seriously on optimizing seal security. Few provide useful instructions on how to effectively use their products. Fewer still arrange for independent vulnerability assessments. Seal developers and manufacturers who do seek independent vulnerability assessments tend to wait until they have a finalized product, when it is too late to make changes. Ideally, vulnerability assessment should be iterative, taking place throughout the seal design and prototyping process[1].

SEALS FOR DISARMAMENT

Seals used for international safeguards, treaty verification, and disarmament require certain unique attributes. In particular, they must deal with one of the classic problems associated with treaty verification: If the inspected facility provides and controls the seals, the inspectors are suspicious that the seals have been tampered with. If, on the other hand, the inspectors provide and control the seals, the inspected facility worries that miniature espionage devices, such as microphones or micro radiation sensors, have been embedded in the seals[23]. The inspected facility may also have safety concerns about allowing foreign hardware near their nuclear weapons.

There are a variety of possible solutions to this problem, but an analysis would go beyond the scope of this paper[24]. It is probably worth speculating here, however, that high-tech electronic seals may be less comfortable to both the inspected facility and the inspectors than quality passive seals because of safety, tampering, and espionage concerns. In any event, seals for use under disarmament treaties require a transparency and negotiability that seals used for other applications do not. No existing seals appear to have been designed with transparency and negotiability much in mind.

Note that seals used for nuclear disarmament treaties will probably have to coexist with seals used for internal security and safeguards. This can be a problem because some weapons containers do not easily accommodate extra seals. Typically, existing weapons containers are often designed more with nuclear safety and ease of use in mind than security.

One important difference between conventional seals and seals used for treaty verification involves the significance of discovering a suspicious seal. If, for example, a suspicious seal is discovered in an internal nuclear security program, that is a very serious matter because it may suggest diversion of nuclear materials. A suspicious seal discovered under a disarmament treaty, however, may be less worrisome. The host (inspected) country will simply not get credit for disarming that particular weapon. The weapon can presumably be taken back to square one and re-entered into the disarmament process.

Finally, seals used under a monitored disarmament treaty often have a psychological and ceremonial role to play, in addition to providing transparency and confidence in the disarmament process. This function is not ordinarily required for internal security and safeguards[25].

SEALS FOR HAZARDOUS WASTE MANAGEMENT

Seals are used surprisingly infrequently for waste management applications, including the storage, handling, and transport of nuclear and other hazardous waste. If used effectively, seals can help to detect and prevent the theft of hazardous materials for terrorist or other purposes. They can also aid in hazardous materials control and accountability, and may help to mitigate legal liability associated with hazardous materials. Seals may protect against sabotage by disgruntled workers or external environmental activists intent on discrediting a waste management program[26]. Seals can also help to detect and prevent inadvertent errors in processing and handling waste containers. Seals will detect malicious or inadvertent tampering with waste data, analysis results, or the calibration or operation of analytical instruments. Seals should have a crucial role to play in detecting unscrupulous efforts to dispose of hazardous waste in containers already certified to contain non- or less hazardous waste.

There are few, if any, existing seals specifically designed or optimized for waste management applications. Seals typically need the following attributes for use on waste containers: robustness, good environmental durability, moderate to high chemical inertness, safety[27], ease of use, and low cost.

One of the difficulties for many waste management applications is the use of metal 55-gallon drums. The drum lid is typically held in place with a circular rim band, clamped with a metal bolt. This is an awkward arrangement for effectively applying a seal. It is also a relatively poor design from the standpoint of container security and tamper detection.

FUTURE SEALS

It seems clear that much better seals are possible. Existing seal designs can, in many cases, be improved with fairly minor modifications if their vulnerabilities are fully understood. New and improved seals are also possible. Seal development by the U.S. Government, however, largely ended in 1993. Some private companies continue to develop new seals, but few (if any) of these are designed for high security, disarmament, or waste management applications.

Novel technologies, materials, and approaches certainly are available to create new and improved seals. These include:

- thin films
- advanced polymers and composites
- exotic organics and macromolecules
- liquid crystals and ferrofluids
- microparticles
- biological materials
- novel glasses
- transport and diffusion phenomena
- ultrasonics
- exotic optical and electrooptic materials
- nano technology
- surreptitious seals
- one-time key pads
- seals combined with human presence detection
- seals combined with biometrics

It may be that the most effective high-security seals in the future will be simple and inexpensive passive designs that are easy to install and interpret, constructed from exotic high-tech materials that are difficult to spoof or counterfeit. Electronic or electrooptic seals are likely to continue to be susceptible to relatively simple attacks, though the level of sophistication required by an adversary is likely to increase.

Improved containers, designed for better security and more effective seal use, are also critically needed. A number of novel technologies and strategies can be exploited to develop better ones.

There is considerable interest in seals that can be interrogated remotely to determine if tampering has taken place. Some commercial seals can now be read from distances of a few meters. For nonproliferation and disarmament purposes, however, remote monitoring from hundreds or thousands of miles away is of interest. It seems likely that even highly sophisticated, remotely monitored seals must be manually inspected from time to time in order to have full confidence that they have not been compromised.

The conventional way that distant seal monitoring is envisioned typically involves the use of encryption, authentication methods, or information barriers. These, however, represent very challenging problems. The use of the most secure encryption or authentication schemes for international verification is unlikely to be permitted due to export control limitations and security concerns. Less sophisticated methods, on the other hand, probably provide inadequate security. Information barriers are, in some ways, even more problematic because they involve the complex interaction of physical and electronic systems that can have a multitude of possible vulnerabilities. It is also difficult to make information barriers compatible with counter-espionage, negotiability, and transparency concerns. We hope to discuss in a future paper some possible ways around these problems[24].

ACKNOWLEDGMENTS AND DISCLAIMER

This paper was prepared under the auspices of the United States Department of Energy. The views expressed herein are those of the author and do not necessarily reflect any official position of Los Alamos National Laboratory. Anthony Garcia, Eric Gerdes, Janie Enter, Eric Baca, Ron Martinez, Jim Doyle, and Jeff Miller provided useful input.

NOTES AND REFERENCES

1. Roger G. Johnston, “Effective Vulnerability Assessment of Tamper-Indicating Seals,” *Journal of Testing and Evaluation* **25** (1997), pp. 451-455, available at http://lib-www.lanl.gov/la-pubs/00418792.pdf

2. Roger G. Johnston, “The Real Deal on Seals,” *Security Management* **43** (1997), pp. 93-100, available at http://lib-www.lanl.gov/la-pubs/00418795.pdf; Roger G. Johnston, “Tamper Detection Requires Dedication,” *Metering International* , issue 3, (1999), available at http://lib-www.lanl.gov/la-pubs/00460170.pdf or http://www.metering.com

3. McGuire Gibson and R.D. Briggs (editors), *Seals and Sealing* (Malibu, California; Bibliotheca Mesopotamica, 1977); Dominique Collon, *First Impressions: Cylinder Seals in the Ancient Near East* (London, England; University of Chicago Press, 1987); Dominique Collon, *Near Eastern Seals* (Berkeley, California; University of California Press, 1990).

4. Denise Schmandt-Besserat, *Before Writing: Volume I: from Counting to Cuneiform* (Austin, Texas; University of Texas Press, 1992), especially pp. 184-199; I.J. Gelb, *A Study of Writing* (Chicago, Illinois; University of Chicago Press, 1963).

5. Lead seals consist of a small piece of lead often with holes for the passage of the sealing wire or string. The wire (or string) is passed through the closure hasp on the container or door to be sealed, or else (in ancient times) it was wrapped around a rolled document. The wire (or string) is then passed through the lead or the holes in the lead, prior to compressing the lead to embed the wire (or string). Often a logo or serial number is embossed into the lead when it is compressed. In recent years, lead seals have fallen out of favor because of their poor security and because of the cost and health/environmental hazards associated with lead. The U.S. Department of Defense (DoD) now prohibits the installation of new lead seals at DoD facilities. Lead seals, however, are still in widespread use in the U.S. and Russia. Sometimes a soft, non-lead alloy is used in place of lead. Such a seal may still be (misleadingly) called a “lead seal” or “lead-wire seal”.

6. E. Porada, “Forged North Syrian Seals,” *Archaeology* **10** (1957), p. 143; E. Porada, *True of False? Genuine and False Cylinder Seals at Andrews University,* Andrews University Seminar Series 6 (Berrien Springs, Michigan; Andrews University, 1978).

7. Ann Waldron, *True or False?: Amazing Art Forgeries* (Norwalk, Connecticut; Hastings House, 1983), p. 11.

8. An **intrusion alarm** or **burglar alarm** can be thought of as an active seal that reports unauthorized entry or access in real-time, rather than recording it for later discover.

9. David L. Poli, *Security Seals Handbook*, Report SAND78-0400 (Albuquerque, New Mexico; Sandia National Laboratories, 1983); *Antipilferage Seal User's Guide*, (Port Hueneme, California; Naval Facilities Engineering Services Center, 1997).

10. *DoD Training Course for Effective Seal Use*, (Port Hueneme, California; Naval Facilities Engineering Services Center, 1999).

11. Roger G. Johnston and Anthony R.E. Garcia, “Vulnerability Assessment of Security Seals,” *Journal of Security Administration* **20** (1997), pp. 15-23, available at http://lib-www.lanl.gov/la-pubs/00418796.pdf; Roger G. Johnston and Anthony R.E. Garcia, “Physical Security and Tamper-Indicating Devices,” *Proceeding of the Information Privacy, Security, and Data Integrity 1997 Mid-Year Meeting,* Gregory B. Newby, ed., (Scottsdale, Arizona; American Society for Information Science,1997), pp. 43-46, available at http://lib-www.lanl.gov/la-pubs/00418767.pdf

12. *Security Seals for the Protection and Control of Special Nuclear Material*, AEC Regulatory Guide 5.15, (Washington, D.C.; Atomic Energy Commission, 1974); Cesar A. Sastre, *The Use of Seals as a Safeguards Tool*, Report BNL 13480, (Upton, New York; Brookhaven National Laboratory, 1969); James L. Jones, *Improving Tag/Seal Technologies: The Vulnerability Assessment Component*, Report 95/00599, (Idaho Falls, Idaho; Idaho National Engineering Laboratory, 1996); Ross J. Anderson and Markus G. Kuhn, “Low Cost Attacks on Tamper Resistant Devices,” *Proceedings of the 5th International Workshop on Security Protocols*, M. Lomas, *et al.*, eds., (Paris; Springer Verlag, 1997), pp. 125-136.

13. We define an individual as being "well-practiced" at a particular attack if: (1) He has recently practiced the full attack at least 8 times AND (2) He has recently practiced the most difficult or critical part(s) of the attack at least 12 times AND (3) working with reasonable haste, he can complete 3 consecutive attacks such that 2 or 3 of them are highly unlikely to be detected using the relevant inspection protocol. For the most difficult attacks, over 50 attempts may be required to achieve criterion (3). Note that it is not necessary to become "well-practiced" to be successful at an attack, just to achieve the defeat times discussed in this paper. For some attacks, an assistant can decrease the attack times considered here. In other cases, however, an assistant just gets in the way. Note also that the number of unused seals needed to become "well-practiced" is not necessarily large. Depending on the attack and on the seal, it is often possible to reuse a seal, or to practice on used seal parts.

14. The marginal cost is the cost to defeat a second seal of the same type. The average marginal cost was much less than $55 because the tools and supplies needed for attacking a particular seal could often be reused for additional attacks on the same type of seal.

15. It is not, in fact, necessary even to exactly counterfeit the original seal. There are an enormous number of configurations of electrons, protons, and neutrons that are close enough to the original that the microscopic discrepancies will go unnoticed. In fact, the original seal itself has a continually changing configuration

due to thermal motion, aging, and light absorption. This allows even more slop in the design of the counterfeit seal.

16. See, for example, the hundreds of references about counterfeiting contained in Roger G. Johnston, *Physical Tampering and Counterfeiting: a research guide* (Chicago, Illinois; American Library Association, 1999).

17. Roger G. Johnston and Anthony R.E. Garcia, *An Annotated Taxonomy of Tag and Seal Vulnerabilities*, Report LAUR 98-5158 (Los Alamos, New Mexico; Los Alamos National Laboratory, 1999). This report also identifies 27 different types of personnel who can engage in an attack, including both insiders and outsiders.

18. See, for example, C.A. Roper, *The Complete Book of Locks and Locksmithing* (Blue Ridge Summit, Pennsylvania; Tab Books, 1983), especially pages 238-251 and the video *B and E: A to Z* (Boulder, Colorado; Paladin Press, 1990).

19. A missing lock is a special case of being unlocked.

20. In a commercial setting, “hassle” might equally well be defined as the economic resources (time, personnel, supplies, equipment) involved in executing the chosen seal protocols. In a government setting, however, with its artificial economics, the term “hassle” may be more appropriate. It may also more accurately reflect the psychological issues associated with seal use that so strongly impact seal effectiveness.

21. The recommendation to show seal inspectors how to defeat the seals they are using is controversial. Some security managers do not want relatively low-level security personnel to be given specific vulnerability information. In the view of the VAT, however, disloyal or incompetent seal installers or inspectors can easily compromise a tamper detection program even without such information. In most cases, the potential benefits of having knowledgeable inspectors far outweigh the risks. For treaty inspections, of course, each side would want its own inspectors to be aware of seal vulnerabilities, but might not wish to share this information with the other side.

22. Richard Feynman has amusingly highlighted the "shoot the messenger" problem that often occurs when security vulnerabilities are uncovered: Edward Hutchings (Editor), Ralph Leighton, Richard Phillips Feynman, and Albert Hibbs, '*Surely You are Joking, Mr. Feynman': Adventures of a Curious Character* (Batam, New York, 1985), pp. 119-137.

23. If one country involved in a treaty fears that the other side has a technological advantage, these worries become even greater.

24. Los Alamos National Laboratory is preparing a paper that discusses some novel, highly negotiable approaches to START III protocols, including unconventional ways to use seals and to remotely interrogate them.

25. Given the poor execution shown by some seal users, even for critical applications, “ceremonial” may nevertheless be an apt description!

26. See R.G. Johnston and A.R.E. Garcia, “Tamper Detection for Waste Managers,” *Proceeding of Waste Management ‘99* (Tucson, Arizona; WMI), CD-ROM, available at http://lib-www.lanl.gov/la-pubs/00418763.pdf. Attacks by disgruntled workers and by outsiders wishing to discredit a waste management operation do not seem to be fully considered in security planning for some waste management programs.

27. Safety is an important issue for certain seal applications. Wire or cable loop seals on moving containers can gouge eyes or skin or catch fingers as they move past facility personnel. Metallic seals sometimes have sharp edges or burrs that can cut skin. They can also become hot from sitting in the sun, or painfully cold in winter. Spark resistance may be an important issue for waste management applications involving flammable or explosive chemicals.

APPENDIX A - A TAXONOMY OF SEAL ATTACKS

The Vulnerability Assessment Team at Los Alamos National Laboratory has developed a taxonomy of different types of general seal attack methods. These 105 different generic attacks fall into the following 11 broad categories:

Failure Mode (Type F) Attacks: challenge the seal security program directly or with misdirection to see if it errors in detecting tampering. Alternatively, wait until an error is made and then exploit it.

Pick (Type P) Attacks: pick the seal so that it opens without damage or any evidence of being opened. Picking works quite well on a surprising number of seals.

Unsealing (Type U) Attacks: unseal (open) the seal, then repair or hide any damage or any evidence of it being opened. This is done before and/or after reattaching the seal. These types of attacks can be very effective, especially if a thorough postmortem exam is not undertaken by the seal user.

Tampering with the Seal Data (Type D) Attacks: tamper with data (such as the seal serial number), or reports and interpretations about the seal inspection.

Tampering with the Seal Reader or Verifier (Type V) Attacks: tamper with the reader (verifier) for seals that rely on an electronic or optical reader to check for tampering.

Sabotaging the Sealing Process (Type S) Attacks: use an insider or outsider to compromise the sealing process.

Backdoor (Type B) Attacks: put a defect in the seal prior to use that can be exploited at a later time. This “backdoor” can be put in during the design or manufacturing process, during shipping or storage, or just prior to use.

Replicating (Type R) Attacks: use the factory to make a duplicate seal using a variety of possible methods including breaking and entering, surreptitious methods, bribery, coercion, or social engineering.

Counterfeiting (Type C) Attacks: the adversary makes a duplicate seal outside of the factory, perhaps starting from new seals or used seal parts.

Electronic (Type E) Attacks: for electronic seals, attack various components such as the sensors, microprocessor, signals, power source, annunciator, or stored alarm condition.

Miscellaneous or Alternate (Type A) Attacks: use a variety of other methods.

FIGURE CAPTIONS

Figure 1: Examples of some commercial passive seals. Top row, left to right: a metal ribbon seal often used on railcars, two plastic strap seals, a bolt (barrier) seal, a plastic bolt seal, and a cable seal. The first 3 seals are open; to close them, one end is inserted into the other. Center: three wire loop seals, including the "e-cup" (left-most of the three) traditionally used in nuclear applications. Bottom row, left to right: two "padlock" seals (which despite the name are seals, not locks), a passive fiber optic seal, and two adhesive label seals.

Figure 2: A schematic tradeoff curve for a typical seal. The more work the user puts into using the seal, the more difficult it is for an adversary to defeat it. The sharp dip in the curve is due to implementation of a postmortem exam after the seal is removed. Though the rest of the curve is drawn smoothly, a magnified view would typically show a series of small stair steps--each small drop representing the introduction of a new procedure into the seal protocol.

Figure 3: Typical tradeoff curves for low-tech vs. high-tech seals (including seals that use high-tech readers). While the high-tech seal can provide better tamper-detection, you often must actually do more work, not less, to achieve the higher security.

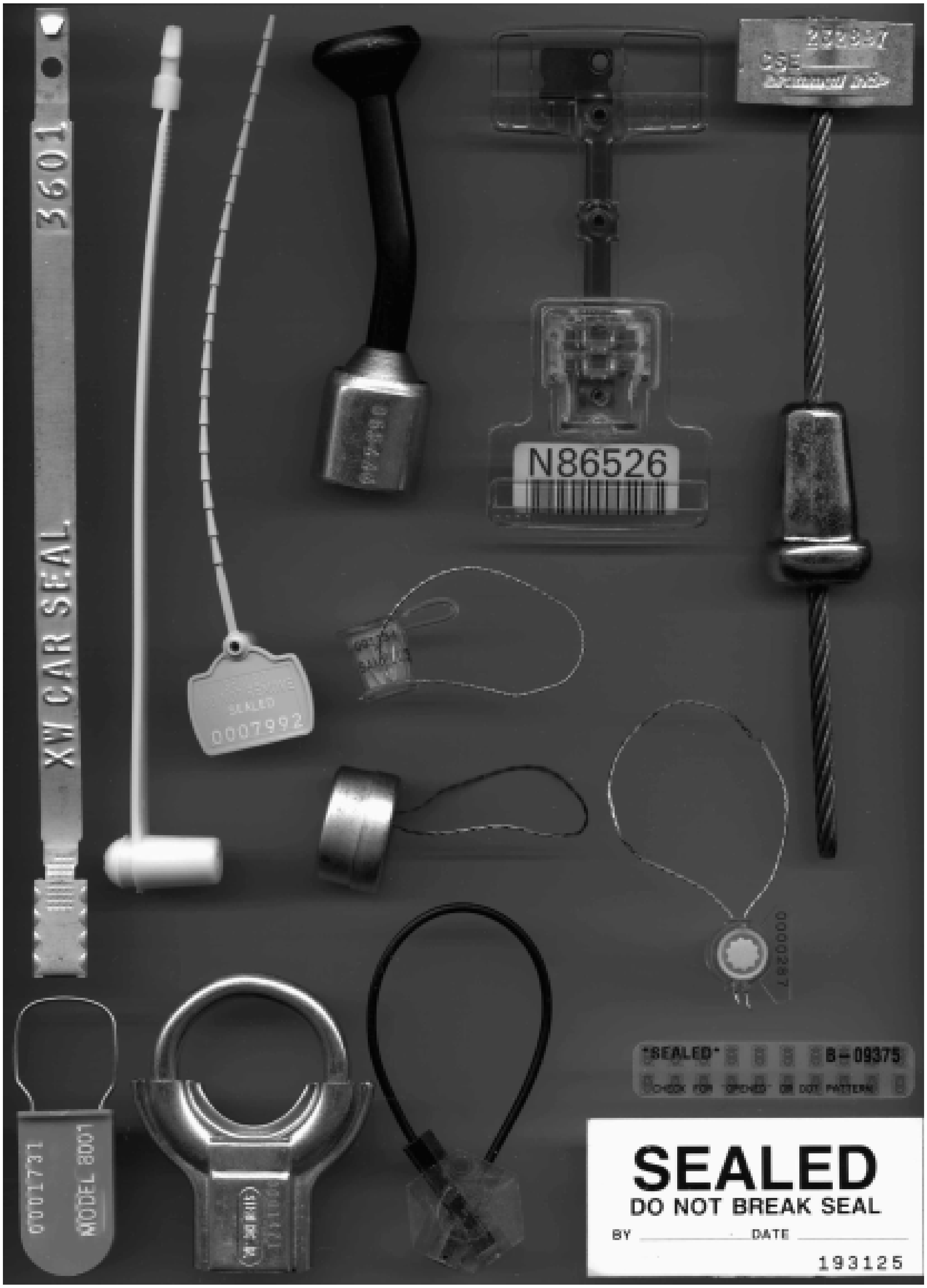
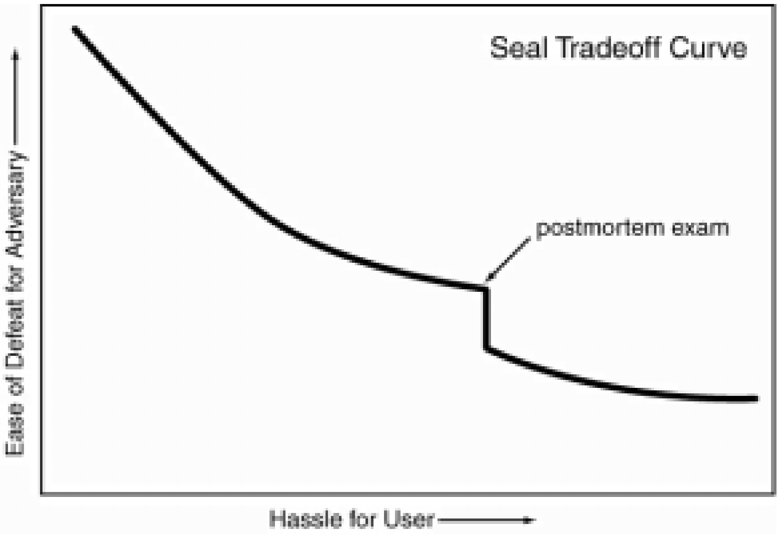

3601
XW CAR SEAL
SEALED
0007992
N86526
0000267
SEALED
B-09375
CHECK FOR "OPENED" OR DOT PATTERN
SEALED
DO NOT BREAK SEAL
BY
DATE
193125
0001731
MODEL 8001

Figure 1



Seal Tradeoff Curve
postmortem exam
Ease of Defeat for Adversary
Hassle for User

Figure 2

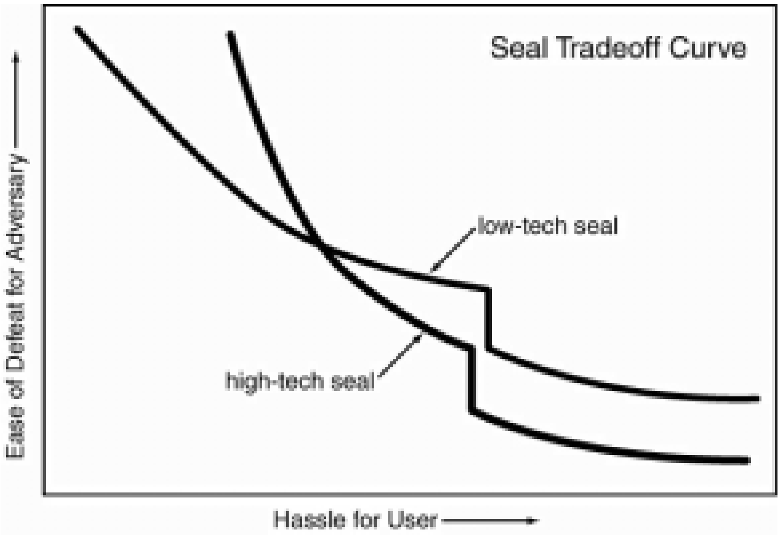

Seal Tradeoff Curve
low-tech seal
high-tech seal
Ease of Defeat for Adversary
Hassle for User

Figure 3